DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY
REFER TO: Network Services (NS3) 10 May 2010

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Department of Defense (DoD) Unified Capabilities (UC) Approved Products List (APL) approval of the Extreme Networks BlackDiamond 8806 Release (Rel.) 12.3.1 Tracking Number (TN) 0904202 as Assured Services Local Area Network (ASLAN) Access (A), Core (C), and Distribution (D) switch.

Reference: (a) DoDI 8100.3, “DoD Voice Networks,” 16 Jan 2004.

1. DoD UC APL approval of the Extreme Networks BlackDiamond 8806 Rel. 12.3.1 TN 0904202 as ASLAN – A, C, and D switch has been granted. This solution achieved Information Assurance (IA) Accreditation from the Defense IA/Security Accreditation Working Group (DSAWG) via e-Vote on 4 Mar 2010. This solution achieved Interoperability Certification (IOC) on 30 Apr 2010 from the Joint Staff (JS). This approval is effective upon the date of this memorandum and expires **4 Mar 2013** unless a critical issue is identified that invalidates either the Interoperability or the IA posture of this product as determined by the JS or the Defense Information Systems Network (DISN) Designated Approving Authority (DAA). Please note that Services and Agencies are required to recertify and reaccredit their systems every three years. Please refer to the UC APL for official posting of this solution at the following URL: http://jitc.fhu.disa.mil/apl/index.html.

2. This product/solution must be implemented only in the configuration that was tested and approved. When the system is deployed into an operational environment, the following security measures (at a minimum) must be implemented to ensure an acceptable level of risk for the sites’ DAA:

a. The site must register the system in the Systems Networks Approval Process (SNAP) Database https://snap.dod.mil/index.cfm as directed by the DSAWG and the Program Management Office (PMO).

b. The configuration must be in compliance with the Extreme Networks military-unique features deployment guide.

c. The system should use a Remote Authentication Dial-In User Service (RADIUS) server or device for authentication when connected to the network.

d. The site should use a SysLog device for auditing purposes when networked.

3. The IOC letter containing detailed configuration on this product will be available at the following URL:
http://jitc.fhu.disa.mil/tssi/cert_pdfs/extreme_blackdiamond_8810_8806_12_3_1.pdf

4. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contained the approved configuration and deployment guide for this solution must

be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO).
E-Mail: ucco@disa.mil
UCCO Process Questions: (520) 538-3234 DSN 879
UCCO Process Manager: (703) 365-8801 ext. 534

SHOWERS.JESSIE
.L.JR.1119211235

Digitally signed by
SHOWERS.JESSIE.L.JR.1119211235
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=DISA,
cn=SHOWERS.JESSIE.L.JR.1119211235
Date: 2010.05.10 18:14:33 -04'00'

JESSIE L. SHOWERS, JR.
Chief, Real Time Services Division